REMARKS

Claims 1-7 all the claims pending in the application, are rejected. Claim 6 is amended.

New claims 8-10 are added.

Claim Rejections under 35 U.S.C. § 112

Claim 6 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. This rejection is traversed for at least the following reasons.

The Examiner states that Claim 6 recites the limitations "said first interface," and "said second interface," at page 14 lines 26-31 of the PCT article 34 amendments filed January 17, 2006. As a result, the Examiner states that there is insufficient antecedent basis for this limitation in the claim.

Applicants have amended claim 6 so that proper antecedent basis is established, and respectfully request that the Examiner withdraw the 35 U.S.C. § 112, second paragraph rejection.

Claim Rejections under 35 U.S.C. § 103

Claims 1-7 are rejected under 35 U.S.C. 103(a) as being obvious over Hearn et al. (US 2005/0091522) in view of Jackson (EP 0911738 A2). Applicants traverse this rejection because the cited prior art fails to disclose or suggest the claim limitations.

Claim 1

Claim 1 recites, *inter alia*:

> ". . . a memory that includes program data executable on said computing device to perform user authentication. . .
> . . . said encryptor is operable to encrypt on the fly data received from said interface and to forward said data once encrypted to said data storage and to decrypt on the fly data received from said data storage and to forward said data once decrypted to said interface."

Hearn

The Examiner alleges that CPU 13 of Hearn corresponds to the computing device of claim 1 and that the Flash ROM 41 of Hearn corresponds to the memory of claim 1. *See* pages 2-3 of Office Action. Applicants respectfully disagree.

Hearn discloses a computer system 11 including a CPU 13, a data bus 15, interface logic 31, a security device 35, and a storage device 21. *See* Hearn, fig. 1. The security device 35 includes a flash ROM 41 which intercepts and controls the computer system's boot process and provides authentication with a login ID and password before access to storage media 21. *See* Hearn, pg. 5, p[0104], p[0108] That is, Hearn discloses a flash ROM 41 residing in the security device 35, which provides authentication for access to storage media 21. The CPU 13 is not involved with the authentication process. Therefore, Hearn fails to disclose or suggest "a memory that includes program data executable on said computing device to perform user authentication" as recited in claim 1.

Hearn also discloses CPU 37, which resides in security device 35, executes the operating system of the security device and communicates with logic 43 that intercepts communications between the host 13 and storage media 21. *See* Hearn, pg. 5, p[0106]. There is no connection to an interface that performs the functions, as claimed.

Notably, the media interface 45 is interposed between the bus control and logic 43, but is expressly disclaimed as an aspect of the invention and is not discussed further (see paragraph [106]) Therefore, even if the CPU 37 is considered the claimed "computing device" it would not

meet the claim requirement for "a memory that includes program data <u>executable on said</u> <u>computing device</u> to perform user authentication" as recited in claim 1.

Further, the Examiner concedes that Hearn fails to disclose or suggest the encryptor as recited in the above reproduced portion of claim 1. *See* page 3 of Office Action.

<u>Jackson</u>

To cure this deficiency, the Examiner alleges that Figure 2, element 4 and paragraph 8 of Jackson discloses this portion of claim 1. *See* page 3 of Office Action. In particular, it appears that the Examiner is alleging that the Data Encryption Device (DED) corresponds to the encryptor of claim 1, and it would have been obvious to combine the encryptor of claim 1 with the disclose computer system of Hearn to disclose the features of claim 1. Applicants respectfully disagree.

Jackson discloses a Data Encryption Device (DED) 4 which encrypts and decrypts data provided to the device. *See* p[0030], col. 7, lns. 57-58. In order to do so, the DED must be enabled by a sixteen ASCII character string, or Crypto Variable (CV), provided to directly to the DED. *See* Jackson, p[0030], col. 8, lns. 2-5. The DED is able to operate in Electronic Code Book (ECB) or Chain Block Ciphering (CBC) mode. *See* Jackson, p[0031], col. 8, lns. 14-19. In ECB mode, the CV must be loaded and the DED will verify that the CV is valid. *See* Jackson, p[0031], col. 8, lns. 20-32. Then the CV is used to encrypt and decrypt data. *See* Jackson, p[0031], col. 8, lns. 20-32. In CBC mode, the CV and an Initialization Vector (IV), which is a higher level of security, must be loaded and the DED will verify that the CV and IV are valid. *See* Jackson, p[0031], col. 8, lns. 33-47. Then, both the CV and IV are used to encrypt and

decrypt the data. *See* Jackson, p[0031], col. 8, lns. 33-47.   In summary, in order for data to be encrypted in Jackson, a CV or CV and IV *must be* provided to the DED.

If the system of Hearn were modified on the basis of the teachings of the DED of Jackson, authentication of the user is performed by the DED, i.e., the encryptor, in addition to the program of Hearn.   This arrangement would, thus, prevent encryption and decryption in real-time, or on the fly, because the DED must receive and authenticate a CV or a CV and IV *before* accessing data to encrypt or decrypt.   Therefore, Hearn in view of Jackson fails to disclose or suggest "said encryptor is operable to encrypt on the fly data received from said interface and to forward said data once encrypted to said data storage and to decrypt on the fly data received from said data storage and to forward said data once decrypted to said interface" as recited in claim 1.

For at least these reasons, Applicants respectfully submit that claim 1 is patentable over the cited prior art.

Claims 4 and 6

To the extent that independent claims 4 and 6 recite subject matter similar to that of claim 1, Applicants respectfully submit that claims 4 and 6 are also patentable over the cited prior art.

Claims 2, 3 and 5

Further, due to their dependency on claims 1 and 4, Applicants respectfully submit that claims 2-3 and 5 are patentable over the cited prior art.

Moreover, as to claim 2, the claim expressly recites:

> "A device as claimed in claim 1, wherein said control system is configured
> to reboot said computing device after successful user authentication and before
> exposing said encryptor to said interface."

8

The Examiner alleges that paragraphs 143 through 145 of Hearn disclose the features of claim 2. *See* page 4 of Office Action. In particular, the Examiner alleges that Hearn's disclosure of an operating system of the security device 37 signals the authentication application program that the security device bus control and interface logic is configured to adopt the data access profile of the user, whereupon the application program at 121 issues the software interrupt vector to the host CPU 13 invoking a warm boot corresponds to the features of claim 2. *See* page 4 of Office Action. Applicants respectfully disagree.

As conceded by the Examiner on page 3 of the Office Action, Hearn fails to disclose or suggest an encryptor. Therefore, Hearn fails to disclose or suggest "wherein said control system is configured to reboot said computing device after successful user authentication and before exposing said encryptor to said interface" as recited in claim 2.

Further, with respect to claim 1, the Examiner relies on Jackson for the teaching of the encryptor. Assuming *arguendo*, that Jackson is combinable with Hearn, the combination of Jackson and Hearn fails to disclose or suggest "wherein said control system is configured to reboot said computing device after successful user authentication and ***before* exposing said encryptor to said interface**" as recited in claim 2 because Jackson in addition requires authentication of a CV or a CV and IV before allowing access to data for encryption and decryption by the DED.

For at least these reasons, Applicants respectfully submit that claim 2 is patentable over the cited prior art.

Accordingly, Applicants respectfully request that the Examiner withdraw the 35 U.S.C. § 103(a) rejection.

New Claims

Applicants respectfully submit that new claims 8-10 are patentable over the cited prior art at least for their recited subject matter and dependency upon claim 1.

Conclusion

In view of the above, reconsideration and allowance of this application are now believed to be in order, and such actions are hereby solicited. If any points remain in issue which the Examiner feels may be best resolved through a personal or telephone interview, the Examiner is kindly requested to contact the undersigned at the telephone number listed below.

The USPTO is directed and authorized to charge all required fees, except for the Issue Fee and the Publication Fee, to Deposit Account No. 19-4880. Please also credit any overpayments to said Deposit Account.
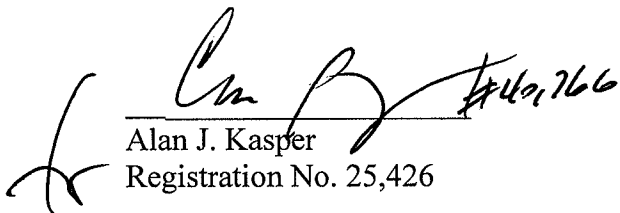
Respectfully submitted,

SUGHRUE MION, PLLC
Telephone: (202) 293-7060
Facsimile: (202) 293-7860

WASHINGTON OFFICE
23373
CUSTOMER NUMBER

Date: April 10, 2009

Alan J. Kasper
Registration No. 25,426